

VTT Technical Research Centre of Finland

Prolonged available time and safe states - State of the art review

Tyrväinen, Tero; Karanta, Ilkka; Kling, Terhi; Sparre, Erik; Authén, Stefan; He, Xuhong; Olofsson, Frida; Bäckström, Ola; Massaiu, Salvatore; Eriksson, Carl; Cederhorn, Erik

Published: 31/10/2019

Document Version
Publisher's final version

License
Unspecified

[Link to publication](#)

Please cite the original version:

Tyrväinen, T., Karanta, I., Kling, T., Sparre, E., Authén, S., He, X., Olofsson, F., Bäckström, O., Massaiu, S., Eriksson, C., & Cederhorn, E. (2019). *Prolonged available time and safe states - State of the art review*. VTT Technical Research Centre of Finland. VTT Research Report No. VTT-R-00883-19



VTT
<http://www.vtt.fi>
P.O. box 1000FI-02044 VTT
Finland

By using VTT's Research Information Portal you are bound by the following Terms & Conditions.


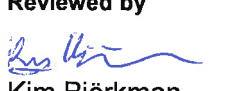

I have read and I understand the following statement:

This document is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of this document is not permitted, except duplication for research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered for sale.

Prolonged available time and safe states - State of the art review

Authors: Tero Tyrväinen, Ilkka Karanta, Terhi Kling, Erik Sparre, Stefan Authén, Xuhong He, Frida Olofsson, Ola Bäckström, Salvatore Massaiu, Carl Eriksson, Erik Cederhorn

Confidentiality: Public

Report's title		
Prolonged available time and safe states - State of the art review		
Customer, contact person, address		Order reference
VYR, NKS, NPSAG		SAFIR 3/2019
Project name		Project number/Short name
New developments and applications of PRA		122529/NAPRA
Author(s)		Pages
Tero Tyrväinen, Ilkka Karanta, Terhi Kling, Erik Sparre, Stefan Authén, Xuhong He, Frida Olofsson, Ola Bäckström, Salvatore Massaiu, Carl Eriksson, Erik Cederhorn		37/5
Keywords		Report identification code
Probabilistic safety assessment, safe state, success criteria, long mission time, human reliability analysis		VTT-R-00883-19
Summary		
<p>This report presents a state of the art review on long time windows in PSA and important related topics. The report consists of the results of a literature review and a questionnaire for the stakeholders of the NPSAG project 53-003 PROSAFE. Topics covered in the report include safe, stable state; success criteria; mission times; recoveries and repairs; HRA methods; risk and reliability analysis methods; reliability data; and epistemic uncertainty. The literature related to long time windows appears to be very limited, because PSA is typically limited to the mission time of 24 hours. Scenarios with long mission times are generally recognized as a challenging area that needs to be studied more.</p> <p>Answers to the questionnaire highlight spent fuel pool accidents and human reliability analysis in long mission time scenarios as important topics to be studied. Longer time windows also bring in the need to model repairs that are usually neglected in normal scenarios with mission time of 24 hours. Modelling of different time windows and time-dependent success criteria could also make PSA models more realistic. In addition, there has been some concern over the applicability of normal failure data to long mission time scenarios.</p> <p>There is significant variety in both the definitions of safe, stable end state found from the literature, and the questionnaire answers concerning the definition and its application. More consistent and realistic consideration of safe end states could improve PSA analyses, e.g. by making mission times and success criteria more realistic, but it is not considered the most important development area according to the questionnaire answers.</p>		
Confidentiality		Public
Espoo 21.10.2019		
Written by	Reviewed by	Accepted by
		
Tero Tyrväinen, Research scientist	Kim Björkman, Research scientist	Tarja Laitinen, Vice president
VTT's contact address		
VTT Technical Research Centre of Finland Ltd, P.O. Box 1000, FI-02044 VTT, FINLAND		
Distribution (customer and VTT)		
SAFIR2022 RG2 members, VTT archive, PROSAFE project partners and stakeholders		
<p><i>The use of the name of VTT Technical Research Centre of Finland Ltd in advertising or publishing of a part of this report is only permissible with written authorisation from VTT Technical Research Centre of Finland Ltd.</i></p>		

Preface

The work presented in this report is part of the PROSAFE project initiated by the Nordic PSA group and financed by Nordic nuclear safety research, The Finnish Research Programme on Nuclear Power Plant Safety 2019 - 2022, Ringhals AB, Forsmarks Kraftgrupp AB, SKB and SSM. The project partners and contributors of this report include Risk Pilot AB, Lloyd's Register Consulting - Energy AB, VTT Technical Research Centre of Finland Ltd and IFE Halden.

Espoo 18.10.2019

Authors

Contents

Abbreviations	4
1. Introduction.....	6
2. Literature review	6
2.1 Safe, stable state	6
2.2 Success criteria	9
2.3 Mission time.....	11
2.4 Crediting recoveries and repairs	12
2.4.1 Modelling and analysis of recoveries and repairs	13
2.4.2 Recoveries and repairs in PSA model.....	15
2.5 Human reliability analysis methods.....	16
2.5.1 Human reliability as a function of time.....	16
2.5.2 Longer time windows	19
2.6 Risk and reliability analysis methods.....	20
2.7 Reliability data	21
2.8 Epistemic uncertainty.....	23
3. Questionnaire	26
3.1 Safe, stable state	26
3.2 Success criteria	27
3.3 Mission times.....	28
3.4 Recoveries and repairs	29
3.5 HRA methods	29
3.6 Methods to model time-dependencies	30
3.7 Reliability data	31
3.8 Epistemic uncertainty.....	31
3.9 Analysis cases to study within the project	31
4. Conclusions	31
References.....	34
Appendix: Questionnaire	38

Abbreviations

Acronym	Description
ASEP	Accident Sequence Evaluation Program
BWR	Boiling Water Reactor
CBDT	Cause Based Decision Tree
CDF	Core Damage Frequency
EDG	Emergency Diesel Generator
EOP	Emergency Operating Procedure
ERO	Emergency Response Organization
FTR	Fail To Run
HCR	Human Cognitive Reliability
HEP	Human Error Probability
HFE	Human Failure Event
HPLV	Human Performance Limiting Value
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation and Air Conditioning
I&AB	Initiators and All Barriers
I&C	Instrumentation and Control
IPE	Individual Plant Examination
LERF	Large Early Release Frequency
LOCA	Loss Of Coolant Accident
LPSD	Low Power and ShutDown
MCR	Main Control Room
NPP	Nuclear Power Plant
ORE	Operator Reliability Experiments
POS	Plant Operating State
RPV	Reactor Pressure Vessel
PPE	Personal Protective Equipment
PROSAFE	PROlonged available time and SAFE states

PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSF	Performance Shaping Factor
PWR	Pressurized Water Reactor
RCS	Reactor Coolant System
SSC	Systems, Structures and Components
SSES	Safe and Stable End State
THERP	Technique for Human Error-Rate Prediction
TRC	Time Reliability Curve
TSC	Technical Support Centre

1. Introduction

Probabilistic safety assessment (PSA) models are mostly very simplified with regard to mission times of safety functions, timings of events, recovery of safety functions and repair of components. Typically, a mission time of 24 hours is assumed for most safety functions in level 1 PSA. Longer time windows are considered rarely, except in some level 2 PSAs and spent fuel pool analyses. The Fukushima nuclear power plant (NPP) accident however pointed out that it might be relevant to consider longer time windows in some accident scenarios (Burgazzi et al. 2014).

The mission time of a typical safety system should be the time that the safety system needs to work in order to reach a safe, stable plant state. Therefore, fundamental questions are how the safe, stable state should be defined, and how the definition should be applied in practice. Another important concept is the success criteria of a safety system, the criteria on how the system needs to function so that the safe, stable state is achieved. The success criteria are typically determined based on deterministic plant simulations. The question of safe, stable state definition is as relevant in the context of deterministic analyses as in PSA.

The goal of the project “Prolonged available time and safe states” (the NPSAG project 53-003 PROSAFE) is to study how the safe, stable state should be defined, and whether it is necessary to adjust success criteria and mission times in PSA. It is expected that in some accident scenarios, there is a need to consider longer time windows. Current practice is that with 24 hour time windows, repairs and their effects need not be considered. Longer time windows bring in the need to model and analyse more recovery actions and component repairs, and to revise human reliability analyses (HRA), since such scenarios offer large time margins for human actions. Static event tree and fault tree modelling techniques may also need to be complemented by dynamic methods, and further development of PSA tools may be needed. In addition, the reliability data and uncertainties in longer time windows are worth considering.

This report provides a state of the art review on long time windows and the definition of safe and stable state in PSA. Two main methods of inquiry have been utilized: a literature review and a questionnaire to the stakeholders of the PROSAFE project. Specific topics that are considered include safe, stable state, success criteria, mission time, HRA methods, crediting recoveries and repairs, reliability analysis methods, reliability data, and epistemic uncertainty.

2. Literature review

2.1 Safe, stable state

Several guidance documents provide some sort of a definition for safe stable state, safe state or controlled state. Table 1 presents definitions from different sources. The definitions are typically very short and open for interpretation. Some of the definitions are significantly different from each other. The definition of ASME/ANS RA-S-2009 is based solely on reactor coolant system conditions. Other definitions include criteria on safety functions. The definition in STUK Y/1/2018 is most specific requiring reactor shutdown, low pressure and removal of decay heat. IAEA documents include criteria on core sub-criticality in the definitions.

Table 1: Definitions for safe, stable state.

Source	Definition
ASME/ANS RA-S-2009	Safe stable state: A plant condition, following an initiating event, in which [reactor coolant system] RCS conditions are controllable at or near desired values.
STUK Y/1/2018	<p>Safe state shall refer to a state where the reactor has been shut down and is non-pressurised, and removal of its decay heat has been secured.</p> <p>Controlled state shall refer to a state where a reactor has been shut down and the removal of its decay heat has been secured.</p> <p>Controlled state following a severe reactor accident shall refer to a state where the removal of decay heat from the reactor core debris and the containment has been secured, the temperature of the reactor core debris is stable or decreasing, the reactor core debris is in a form that poses no risk of re-criticality, and no significant volumes of fission products are any longer being released from the reactor core debris.</p> <p>Safe state following a severe reactor accident shall refer to a state where the conditions for the controlled state of a severe reactor accident are met and, in addition, the pressure inside the containment is low enough that leak from the containment is minor, even if the containment is not leak-tight.</p>
IAEA-SSG-2	Typically, it is assumed that a safe and stable end state is achieved when the core is covered and long term heat removal from both the core and the containment is achieved, and the core is, and will remain, subcritical by a given margin.
IAEA-SSR-2/1	<p>Safe state: Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.</p> <p>Controlled state: Plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to effect provisions to reach a safe state.</p>
IAEA-TECDOC-1804	<p>Safe stable state: A plant state, following an initiating event, in which plant conditions are controllable at or near desired values and within the success criteria for maintenance of safety functions. A safe stable state is achieved when the following criteria are met:</p> <ul style="list-style-type: none"> All required safety functions are successfully performed during the defined mission time.

	<ul style="list-style-type: none"> The safety functions are not expected to be lost at a point close-in-time after the specified mission time (i.e. there is compelling evidence that the successful safety functions have adequate operating capacity to be maintained for an indefinite period following the end of the specified mission time, or that there are adequate alternative means of performing the safety functions that can be implemented with high confidence after the specified mission time).
Jacquemain et al. 2018	<p>A plant is considered in a safe stable state when all components of the degraded core are in a coolable configuration, either still in place and/or relocated in-vessel and/or ex-vessel, and any stored spent fuel is also in a coolable configuration. The degraded core, if retained in-vessel, is considered to have reached a coolable configuration when there is no further hydrogen production from water-metal (clad and structural materials) interaction, the release rate of fission products is exceedingly low and there is no risk of re-criticality or of corium rupturing the vessel. Similarly, the degraded core, if ex-vessel, is considered to have reached a coolable configuration when there is no further incondensable gas generation from molten core concrete interaction, release of fission products from core-concrete interactions is exceedingly small, there is no risk of re-criticality and the ex-vessel core debris is retained in the containment without breaching the containment integrity. The spent fuel inventory is considered in a coolable configuration if all the spent fuel rods, degraded or not, are confined in the pool without the risk of a runaway oxidation reaction, there is no significant production of hydrogen and no risk of criticality.</p>
NUREG-2122	<p>Safe stable state: Condition of the reactor in which the necessary safety functions are achieved.</p> <p>In a PRA, safe stable states are represented by success paths in modeling of accident sequences. A safe stable state implies that the plant conditions are controllable within the success criteria for maintenance of safety functions.</p>

Each end point of level 1 PSA should be either a safe, stable state (or at least controlled state) or core/fuel damage state (IAEA-TECDOC-1804). However, the authors have not found any quantitative criteria for safe, stable state from literature, except concerning reactor sub-criticality (effective multiplication factor less than 0.995 in STUK Y/1/2018). Success criteria analyses often consider a fixed time window, typically 24 hours, and it is studied whether core damage occurs during that time window or not given specific conditions (NUREG-1953, Butler et al. 2010). The basis for success criteria seems to be avoidance of core damage within the fixed time window rather than reaching a safe, stable state. For example, NUREG/CR-7177 studies definitions of core damage surrogates for success criteria analysis. The conditions at end points of the analyses are examined to check if the plant is in a stable state or safe stable state, but it is not specified what it exactly means, and the time point where safe stable state is reached is not determined.

Ma & Buell (2016) have studied safe and stable state in event tree modelling with quite similar scope as the PROSAFE project. They have considered the definitions from ASME/ANS RA-S-2009 and NUREG-2122, and have not specified any quantitative acceptance criteria for safe state. They point out the importance of checking the trends of plant parameters, such as core temperature, i.e. are the parameter values stable or changing at the end of a thermal-hydraulic analysis. If the parameter values are steady, the plant state can be assumed safe and stable. If the parameter values are changing, the mission time of the thermal-hydraulic analysis should be increased. In such a case, Ma & Buell recommend a mission time of 72 hours if it is practically possible.

In some PSAs, controlled states are used as end states instead of safe states. ASAMPSA_E (2015) points out the issue that safety analyses should be performed to the point where a controlled plant state is reached. ASAMPSA_E does not provide a definition, but states that it should be “defined by clear criteria for plant parameters and availability of essential safety functions.” It states also that “challenges to such a controlled state should require additional, independent events in PSAs modelling.”

ANS/ASME-58.22-2014 argues that for low power and shutdown (LPSD) PSA, there may be a need to evaluate successful end states of the at-power PSA to examine potential failures during repair and through start-up, e.g. feed and bleed cooling, high pressure recirculation, low pressure recirculation, and states with reactivity controlled but without the control rods inserted. They however conclude that these scenarios are low in frequency and often are neglected.

For severe accidents, the definitions of safe, stable state are more complicated. They also address the conditions related to reactor core debris and its coolability, and the release rate of fission products. The definition in STUK Y/1/2018 concerns also conditions of the containment. Jacquemain et al. (2018) specify also criteria that there should not be significant hydrogen production or core-concrete interaction anymore.

Jacquemain et al. (2018) state that some severe accident management guidelines specify acceptance criteria for a controlled, stable state after a severe accident. The variables used in the criteria include core exit temperature, hydrogen content, the pressure of the containment, radiation levels and the water level of the spent fuel pool. The criteria are however not presented in (Jacquemain et al. 2018).

2.2 Success criteria

The definitions of success criteria from different sources are often similar, e.g. as stated in ASME/ANS RA-Sa-2009: *“Criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied.”* Table 2 presents definitions from different sources.

NUREG-2122 states that PSA uses several different types of success criteria, e.g. for different safety functions, for system functions needed to support the safety functions, and for the components within these systems. The success criteria specify how the systems and components must function, when they must begin to function, and how long they must function.

The success criteria are typically developed by thermo-hydraulic analyses that represent the design and operation of the plant being evaluated, and where deterministic acceptance criteria are defined for the different safety functions.

Normally, success criteria in the PSA are defined relative to the initial requirements when an initiating event has occurred, and rarely take into account the possibility of increased safety margins, and thus less stringent requirements, some time after the initiating event. The time period, i.e. the mission time, during which the specified criteria need to be fulfilled is in most

cases set to 24 hours (PSA level 1) or 48 hours (PSA level 2), even though the required time may be shorter. ASME/ANS RA-Sa-2009 requires for all Capability Categories that the effect of variable success criteria (for system functions) due to time dependence shall be incorporated into the system modelling.

ASME/ANS RA-Sa-2009 requires for Capability Category II that acceptance criteria are chosen such that the determination of core damage is as realistic as possible, and with enough margin to code-calculated values to allow for limitations in the code. Examples of core damage surrogates are given as:

- a. Collapsed liquid level less than 1/3 core height or code-predicted peak core temperature > 2500 °F (1371.1 °C, BWR)
- b. Collapsed liquid level below top of active fuel for a prolonged period, or code-predicted core peak node temperature > 2,200 °F (1204.9 °C) using a code with detailed core modelling, or
code-predicted core peak node temperature > 1,800 °F (982.2 °C) using a code with simplified (e.g., single-node core model, lumped parameter) core modelling, or
code-predicted core exit temperature > 1,200 °F (648.9 °C) for 30 min using a code with simplified core modelling (PWR)

NUREG/CR-7177 also studies definitions of core damage surrogates for success criteria calculations with thermo-hydraulic analysis and defines a peak cladding temperature of 2200°F (1204.9°C) as an appropriate surrogate for core damage at at-power analysis. For shutdown conditions they recommend a combination of surrogates, e.g. a reactor pressure vessel water level of one-third of the fuel height as a precursor to fuel damage and a peak cladding temperature of 1204.85 °C as a precursor to core damage.

ANS/ASME-58.22-2014 states that changes of success criteria during a plant operating state (POS) requires a change in the POS interval and an additional POS to be defined.

Ma & Buell (2016) have addressed the definition of success criteria in their study of safe and stable state, by using the definition of ASME/ANS RA-Sa-2009. They point out the close relation between safe and stable state, mission time and success criteria, and that a success criterion shall include a specified mission time a safety function needs to operate in order for the reactor to reach a safe and stable state. They present an iterative process for developing success criteria that a) "represent the minimum number of systems/components and human actions that are required to ensure the safety function" and b) results in a safe stable state verified by thermo-hydraulic analysis results.

In the aftermath of the Fukushima accident it was recognised that present state-of-the-art PSA contain several insufficiencies, e.g. concerning the consideration of long scenario analysis times and mission times but also concerning that success criteria should be clearly defined for reaching a long term stable end state (ASAMPSA_E 2015). Consideration of partial core damage was also identified to result in the need for development of specific success criteria.

Table 2: Definitions of Success Criteria.

Source	Definition
ASME/ANS RA-S-2009	<p>Success Criteria: Criteria for establishing the minimum number or combinations of systems or components required to operate, or minimum levels of performance per component during a specific period of time, to ensure that the safety functions are satisfied.</p> <p>The term accident success criteria is a technical element in the ASME/ANS PRA Standard whose objectives are to define the plant-specific measures of success and failure that support the other technical elements of the PRA. The minimum combination of systems and components needed to carry out the safety functions given an initiating event.</p>
IAEA-TECDOC-1511	<p>Success criteria regarding the plant response to initiating events are used to specify whether safety related functions meet the requirements to prevent damage to the core or mitigate significant releases of radioactivity. These safety-related functions in terms of a PSA may be functions of operating systems, front line safety systems, I&C, support systems, structures, components, and operator actions. For operator actions success criteria are characterized by statements that certain actions are successfully carried out within a defined time window.</p>
NUREG-2122	<p>The minimum combination of systems and components needed to carry out the safety functions given an initiating event.</p>

2.3 Mission time

ASME/ANS RA-S-2008 defines mission time as “the time period that a system or component is required to operate in order to successfully perform its function.” For many safety functions, the mission time must be the time it takes to bring the plant to a safe, stable state (IAEA-TECDOC-1804). The mission time is however often just set conservatively to 24 hours based on earlier experience without detailed analysis. This approach has been criticised, e.g. in ASAMPSA_E (2015). A more realistic approach is to use suitable deterministic computer code to determine how long it takes to bring the plant to safe state. The mission time analysis is closely connected to success criteria analysis, and e.g. same thermo-hydraulic calculations may be utilised in both analyses.

In a typical PSA, the mission time is 24 hours for most safety functions. The Fukushima accident however demonstrated that it can be relevant and more realistic to consider longer mission times (Burgazzi et al. 2014). For example, in cases of long term station blackout or loss of ultimate heat sink, mission times of 48 hours or 72 hours could come into question.

Shorter mission times than 24 hours have also been considered. Risk assessment of operational events handbook (USNRC 2017b) provides an example that in the case of loss of coolant accident (LOCA), the mission time of low pressure injection could be 1 hour, after which recirculation needs to function 23 hours.

Risk assessment of operational events handbook (USNRC 2017b) states that the mission time of emergency diesel generators has been determined based on the mean recovery time of the offsite power in some PSAs. In the case of loss of offsite power, there are examples of shorter (e.g. 2 hours) and longer mission times (e.g. 72 hours) (WGRISK 2017). 72 hours have been used for containment systems and spent fuel pool analysis.

If a safe, stable state has not been achieved at the end of the mission time, IAEA-TECDOC-1804 recommends one of the following alternatives:

- Assigning an appropriate plant damage state for the sequence,
- Extending the mission time to the point where a safe, stable state is reached,
- Modelling of additional system recovery or operator interactions that bring the plant to a safe, stable state.

As the current best practise, Ma & Buell (2016) recommend 72 hours as the maximum mission time, because the accuracy of the analysis is expected to decrease with longer time windows, and the likelihood that non-modelled mitigation/recovery actions terminate the accident increases. They recommend sensitivity analyses for such scenarios.

If different mission times need to be modelled for the same event in different scenarios, an option is to use different basic events for different mission times in the PSA model. Recovery rules or fault tree configurations management techniques can be used to select the correct basic event for the analysed accident sequence. Use of multiple basic events to represent different mission times can however be somewhat inconvenient e.g. in risk importance measure computation, but it seems that current PSA tools do not offer better options to handle the issue. A possibility to facilitate the modelling could be to develop functionality to select the mission time of a basic event based on the accident sequence.

2.4 Crediting recoveries and repairs

In PSA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems (NUREG/CR-6823).

- Recovery actions involve the use of alternate equipment or means to perform a safety function when primary equipment fails, or the use of alternate means to utilize equipment that has not responded as required. Examples of recovery actions include opening doors to promote room cooling when an HVAC system fails, recovering grid-related losses of offsite power by rerouting power, manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a handwheel to manually open a motor-operated valve when the motor fails to operate.
- Repair actions involve the elimination or mitigation of the faults that caused a component or system to fail, and bringing it to operable state. Examples of repair actions include repairing weather-related losses of offsite power, repair of a pump that failed to start, or replacement of a failed circuit breaker.

There are two main issues in crediting recoveries and repairs in the PSA model:

- How to assess the probability that recovery or repair is successful in a given time window (or more generally, probability distribution of the time that recovery or repair of the system takes).
- How to model recovery or repair of the safety system in the PSA model.

PSA models typically include a number of recovery actions. For example, the recovery of offsite power is a recovery event that has often been modelled in PSA. Recovery of emergency diesel generators has also been modelled in many PSAs (USNRC 2017b). Concerning offsite power, multiple possible recovery times are often modelled (WGRISK 2017).

Because recovery actions can involve complicated actions that are usually governed by procedures, most are typically evaluated using HRA methods. A general exception is the treatment of offsite power recovery where the required recovery actions are often not within the jurisdiction of the plant personnel. Thus, offsite power recovery data is collected for use in PSAs (NUREG/CR-6823).

The repair of components is typically not modelled in PSA because one or more of the following apply to most minimal cut sets and accident sequences (USNRC 2017b): (1) the time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed), (2) repair is an action that is not always governed by procedures and thus difficult to model, (3) the availability of spare parts is not always certain, and (4) abnormal procedures generally direct operators to rather use alternative equipment.

2.4.1 Modelling and analysis of recoveries and repairs

There are three main approaches to analyse recoveries and repairs: the judgmental approach, the statistical approach and the systems approach. In the judgmental approach, an expert or a group of experts assess and give estimates on various quantities of interest. In the statistical approach, the model is derived from available data, with the internal logic of the recovery or repair being of secondary concern. In the systems approach, the recovery or repair is considered to consist of more than one constituent parts (activities), and the model consists of models for the activities and the dependences between them. Also hybrids of two or all three approaches may be used.

There are several types of risk associated with recoveries and repairs, such as performance risk (the repaired/recovered system does not fill its performance requirements), side effect risk (the repair/recovery action compromises some SSCs of the plant), cost risk and occupational health risk, but the main emphasis in PSA has been on schedule risk. This is the risk that the recovery or repair may be completed too late from the accident progression point of view.

In the judgmental approach, various methods to elicit probabilities and other quantities from experts have been developed, and various issues to take into account in the process have been identified (e.g. Ortiz et al. 1991, Cooke 1991, Meyer & Booker 2001, Ayyub 2001, O'Hagan et al. 2006). Humans are notoriously prone to various errors of judgment, and these have to be taken into account in formulating the questions posed to the experts. Also, other issues have to be taken into account, for example that experts are not asked to supply too many estimates. Nevertheless, the judgmental approach is often used when enough data is not available and when a systems model of the repair/recovery cannot or will not be built.

In the statistical approach, the main method used to model the uncertain completion time of an action is to fit a probability distribution to the data. There are many probability distributions that can be used, for example the exponential, normal, Weibull, gamma and lognormal distribution (see, e.g. Bury 1999). The lognormal distribution is often used in the modelling of the duration of human activities, because analysis of data has shown that maintenance times tend to be lognormally distributed (O'Connor & Kleyner 2012 p. 410). Nevertheless, the choice of distribution depends on what kind of activity is being modelled and how well each distribution fits the data available.

Recoveries and repairs are results of human actions. These actions may consist of several interdependent activities, and they may be carried out by more than one person. Thus, there is some justification to consider them as operations (or projects). There are two systems

approaches to the risk analysis of recoveries and repairs: one based on operation or project risk analysis, and one based on human reliability analysis.

One approach to the modelling and analysis of recoveries and repairs as contributors to risk is provided by project risk analysis, although its use in the nuclear safety field seems to have been minor so far (perhaps partly because repairs and recoveries have received relatively little attention). In this approach (Williams 2002), a recovery or repair is viewed as consisting of a set of activities (also called tasks) that have precedence constraints between them and that are performed with some resources (humans, spare parts, materials etc.). The set of activities may be obtained by constructing a work breakdown structure (Norman et al. 2008). In the analysis of schedule risk, the most common quantitative methods are the critical path method (CPM), project evaluation and review technique (PERT), and Monte Carlo simulation of activity networks (Munier 2014). Performance risks have received much less attention than schedule risks, but in principle they can be accounted for by e.g. fault trees.

Risk assessment of operational events handbook (USNRC 2017b) summarizes the following factors from the PRA standard supporting requirements (ASME RA-Sa-2009) which should be considered in the analysis of recovery actions as well as repairs:

- plausibility and feasibility of the action in the analysed scenarios,
- availability of procedures, operator training, cues and manpower,
- scenario-specific performance shaping factors in the HRA,
- dependencies between human failure events in scenarios, accident sequences or minimal cut sets.

The handbook also contains a more detailed list of questions to be considered when modelling recoveries and repairs. In addition, it presents some examples of failure events and potential recovery/repair actions. The list provided by the handbook is not complete, because e.g. the availability of spare parts is not considered.

Risk assessment of operational events handbook (USNRC 2017b) states that HRA techniques for estimating the likelihood of successful repair should not be used. This is because the possible repair scenarios, which are affected by a variety of human actions and hardware-related issues, would not be known without knowing the specific causes of the problem. There are however exceptions, such as the replacement of fuses, which can be performed rather quickly since spare fuses are available. In that case, the failure probability for the repair can be estimated by HRA or statistical analysis based on available repair data.

Existing HRA methods may be subjected to criticism also on the ground that they usually have a too simplistic view on repair time and factors that affect it. Some methods also may be inapplicable due to various reasons: for example, sufficient data might not exist to estimate the parameters of a repair time probability distribution.

Kichline (2018) points out that current HRA methods were not developed to quantify the human error probabilities (HEPs) associated with the transportation, placement, connection, or local control of portable equipment. Existing HRA methods may model certain types of actions and some performance shaping factors similar to those associated with the use of portable equipment. However, the HEPs were not developed for the context of FLEX (flexible coping strategies) actions (e.g., the HEP for a human task in the technique for human error-rate prediction (THERP) might be very different from the HEP of the same task in the scenario that results in the use of FLEX equipment).

Recovery/repair data used in probability estimation should reflect accident conditions (NUREG/CR-6823). Data from non-accident conditions should not be used, because there is

no similar pressure for the performance of the action. NUREG/CR-6823 provides guidance for probability estimation based on operating data.

2.4.2 Recoveries and repairs in PSA model

Recoveries and repairs of safety relevant SSCs, whether successful or not, may significantly change accident progression. Therefore, they need to be considered in the plant PSA model if the mission time is sufficiently long so that recoveries and repairs may credibly take place.

Recoveries/repairs of failure to run events may need to be modelled separately from failure on demand events (USNRC 2017b). If a component works some time before it fails, the time available for recovery/repair can be extended significantly, because the time to core damage is delayed. Failure times are therefore highly relevant when considering recoveries and repairs, and modelling of failure times can affect recovery/repair modelling significantly. However, in PSAs, failure to run events are typically conservatively assumed to occur at the time of the demand.

Another issue is that repair time can depend significantly on the specific failure causes and how the component exactly fails. Accurate repair modelling may therefore require division of a failure basic event into multiple events. For example, failures could be divided into those that can be repaired in a short time and those that require long repair times on the average. This might require re-evaluation of the failure data. The division could be done either explicitly in the PSA model or in background calculations providing inputs for the PSA model.

Recoveries and repairs can be modelled in PSA at the event tree level, fault tree level, sequence level and minimal cut set level (USNRC 2017b). Recoveries from initiating events and main safety functions are typically modelled at the event tree level as additional event tree branches. Recoveries and repairs of individual components and subsystems are usually modelled at the fault tree level. A typical example of fault tree modelling is that the component failure basic event and the failure to recover/repair basic event are set under an AND gate. Scenario-specific basic events can be used for the same recovery/repair event if the probability of the recovery/repair varies depending the scenario. Techniques to handle such cases include recovery rules and use of multiple configurations of the same fault tree. Different fault tree configuration can, for instance, be applied to different accident sequences. Recovery rules can be used to manipulate minimal cut sets (USNRC 2017b).

When the failure of the safety function has a major impact on accident progression, modelling recovery or repair at the event tree level is called for. In the simplest case, the recovery/repair of the component/subsystem/structure may be represented as a section in the event tree. The success criterion of the recovery/repair is that it is completed within some given time frame. If accident progression differs significantly depending on when the recovery/repair occurs, modelling of several time limits can be considered and several branches may be added to the tree in the recovery/repair section. This type of modelling may however make event trees very complicated, and therefore, the conventional event tree/fault tree based modelling approach is not the most suitable method for detailed recovery modelling.

Risk assessment of operational events handbook (USNRC 2017b) states that the recovery and repair modelling should credit only one component in a system if there are multiple failed components. If there are failures in two systems, the possibility to recover/repair both requires case-specific consideration. If one failure can be recovered quickly from the control room, e.g. by simple trip reset, there may be time for another recovery or repair. In the case of multiple recoveries/repairs or recovery/repair combined with other human error events, it is important to analyse the dependencies.

If a component has a large failure probability, it may be relevant to consider second failure after recovery or repair.

Recovery of emergency core cooling systems is sometimes modelled in level 2 PSA (ASAMPSA2 2013). The recovery may also induce additional risk, if the recovery can occur in a critical time window to produce large amounts of hydrogen. Therefore, instead of modelling only success and failure of recovery, modelling of different recovery times may be needed to make the analysis realistic. Recovery time modelling in simulation-based containment event trees has been studied in (Tyrväinen & Karanta 2019).

2.5 Human reliability analysis methods

How to account for available time is an important issue in HRA, especially for the post-initiator human failure events (HFEs) (Category C). Historically the main focus for Category C HRA has been on supporting Level 1 PSA, that is, to estimate the likelihood of the main control room (MCR) operators failing to implement the emergency operating procedures (EOPs) in a number of accident scenarios that might end up in damaging the reactor core. The typical available times for nuclear power plant level 1 human actions are among 30 minutes to 1 or 2 hours. The existing HRA methods are developed to cope with this situation.

It seems that HRA of field workers other than operators (such as maintenance personnel) has not received much attention in HRA literature. Even though pre-initiator (Category A) HFEs are related to the maintenance personnel, they are typically latent errors that the personnel make during normal situations at the plant. Nevertheless, the success or failure of these NPP workers in repair and many recovery activities may affect accident progression significantly in long time window scenarios.

2.5.1 Human reliability as a function of time

Human error probability of a typical Category C HFE includes both diagnosis (e.g. detection, decision making) error probability and execution error probability (IAEA 50-P-10, 1996).

NUREG-1921 (NUREG-1921, 2012) provides a timeline illustration diagram (Figure 1), and shows the definitions of start time, time delay, available time, cognition time, execution time and required time.

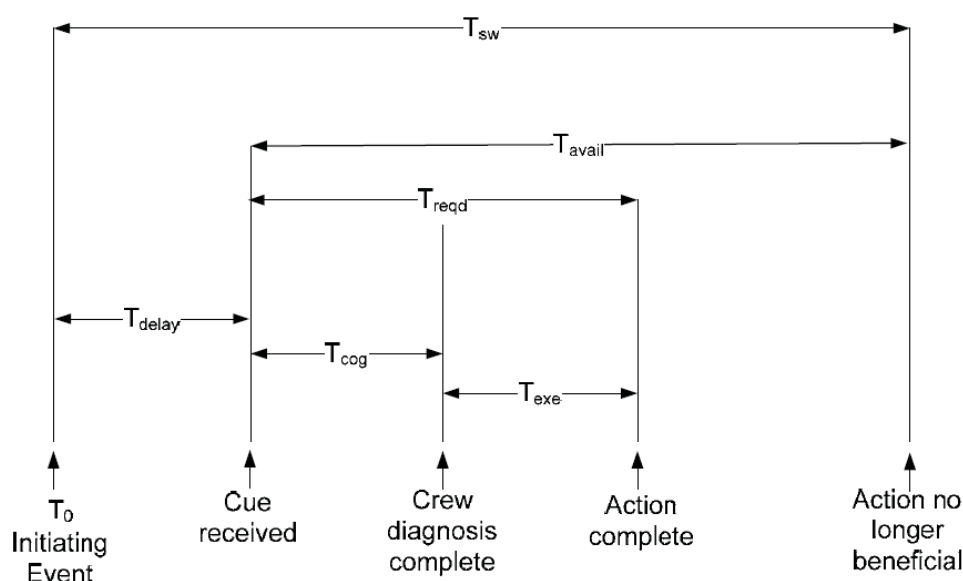


Figure 1: Timeline illustration diagram (NUREG-1921).

The terms associated with each timing element are defined mathematically.

- T_0 = start time = start of the event
- T_{delay} = time delay = duration of time it takes for an operator to acknowledge the cue
- T_{sw} = system time window, is the time from the start of the event until the action is no longer beneficial (typically when irreversible damage occurs, such as core damage or component damage). The system time window represents the maximum amount of time available for the action.
- T_{avail} = time available = time available for action = $(T_{sw} - T_{delay})$
- T_{cog} = cognition time consisting of detection, diagnosis, and decision making
- T_{exe} = execution time including travel, collection of tools, donning personnel protection equipment (PPE), and manipulation of components
- T_{reqd} = time required = response time to accomplish the action = $(T_{cog} + T_{exe})$

In addition to the above terms, time margin is used in several HRA methods. Time margin can be defined as the ratio of time available for the recovery action to the time required to perform the action ($T_{cog} + T_{exe}$) and is calculated as follows:

$$Time\ Margin\ (TM) = \frac{T_{avail} - T_{reqd}}{T_{reqd}} \times 100\%$$

For the diagnosis part, the available time has always been an important factor. Some HRA methods consider time as the dominant factor in diagnosis HEP estimation, e.g. human cognitive reliability (HCR)/operator reliability experiments (ORE) (Parry 1992) or time reliability curve (TRC) in THERP (NUREG/CR-1278, 1983). Some HRA methods consider time as one of the performance shaping factors (PSFs), e.g. SPAR-H (NUREG/CR-6883, 2005).

In general the time reliability curves used in HRA assume that the probability of a human failure event (its cognitive part and execution part) will be lower when the available time is longer. Figure 2 presents the TRC used in THERP for diagnosis HEPs. The nominal median HEP is $1E-4$ for diagnosis of the first initiating event 60 minutes after the event cues (signals) appear in the main control room. The HEP will be lower when the time is longer.

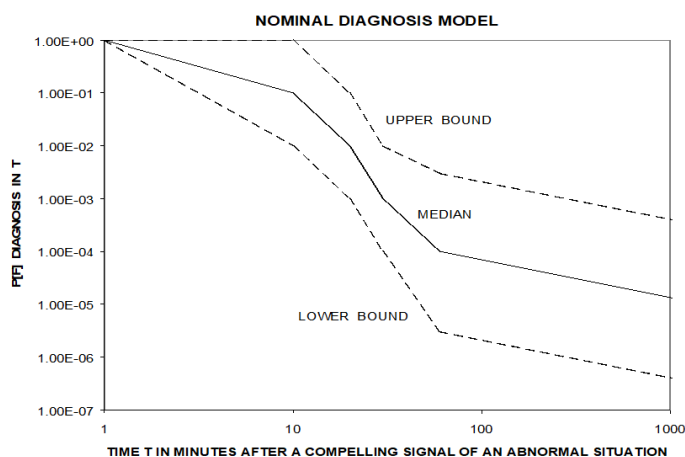


Figure 2: Time reliability curve used in THERP for diagnosis human error probabilities (NUREG/CR-1278).

In SPAR-H the available time is one of the eight PSFs in the HEP estimation. Table 2 shows the multipliers for the available time PSF for LPSD tasks. With the expansive time, the multiplier can be 0.1 to 0.01 for the diagnosis (nominal diagnosis HEP is 1E-2) and 0.01 for the action (nominal action HEP is 1E-3) part of LPSD tasks.

Table 2: Available time performance shaping factor for low power and shutdown (NUREG/CR-6883).

Case	Available time	PSF Multiplier	Notes
LPSD: Available time for diagnosis	Inadequate time	P(failure) = 1.0	<p>* Analyst's choice, depending on complexity of diagnosis, including multiple factors such as available help and likelihood of additional cues.</p> <p>** Analyst's choice, depending on complexity, PPE, work environment and ease of checking and recovery.</p>
	Barely adequate time (approximately 2/3 x nominal)	10	
	Nominal time	1	
	Extra time (between 1 and 2 x nominal)	0.1	
	Expansive time (> 2x nominal)	0.1 to 0.01*	
LPSD: Available time for action	Inadequate time	P(failure) = 1.0	
	Time available is approximately equal to time required	10	
	Nominal time	1	
	Time available is ≥ 5x the time required	0.1	
	Time available is ≥ 50x the time required	0.01**	

There are important issues connected with the use of TRC methods in HRA. The first is the risk that some HRA methods, e.g. HCR/ORE or TRC of THERP, might produce unrealistically low diagnosis HEPs when time is considered as the dominant factor in the estimation/calculation of HEPs for human failure events (HFEs) with longer time frames. To avoid unrealistic estimation of low HEP, NRC (NUREG-1792, 2005) suggests that some limiting HEPs should be defined, considering the uncertainties. In UK, the human performance limiting value (HPLV) is typically set as 1E-5. However, for optimal conditions and scenarios with excessive time scales (> 12 hours) the HPLV can be justified as 1E-7.

The cause based decision tree (CBDT) method was intended to address actions with longer time frames that were outside the valid range of extrapolation for the monotonically decreasing HCR/ORE TRC. CBDT considers a relatively large set of potential PSFs and operator influences (e.g., quality of training, procedures, the human-machine interface, recovery potential) and uses a series of decision trees to establish the HEP. However, CBDT appears to be a method for treating post-initiator control room actions only (guidance and data for quantifying local actions is not provided) through a time-independent quantification approach. In that approach, time is considered qualitatively in addressing the potential for self-recovery of an error or recovery by another crew member. As a result, any analytical (i.e., not based on

plant specific human error data) non time-related HRA method could be used for treating longer time frames in the way CBDT does.

A second issue with TRC methods is that they use time as the main (or only) determinant for the HEP, in which case it works as a proxy cause for the combined effect of all underlying causes of human error or non-response. Concern is raised about using the HCR/ORE and THERP TRC blindly across many different scenarios and contexts without consideration of other factors that may be more dominant error causes, thus arriving at optimistic estimates (NUREG-1842, p. A-2). This is especially serious when plant/context specific data are not collected and generic TRCs are used. The TRC in THERP is based on expert judgment derived from some early simulator data collections by General Physics and Oak Ridge. The TRC of the HCR/ORE was developed by EPRI in a simulator data collection program called ORE to examine the validity of the original HCR curves (Jung & Park 2019). The results of ORE experiments did not support the use of the four factors originally included in the HCR TRCs (i.e., training, human-system interface, experience, stress). The factors were dropped from the HCR/ORE approach (NUREG-1842, p. 3-50) leaving time (available time and crew response time) as the only determinant for the HEP. It is thus an important assumption of the HCR/ORE method that the influence of important plant-specific factors will be implicitly included in the simulator-based, time-to-respond data that is collected at the plant and/or in the plant-specific estimates obtained from operators (NUREG-1842, p. 3-51).

2.5.2 Longer time windows

Most reference sources for HEPs are typically about main control room operating crews' tasks performed in a relatively short period of time (e.g., THERP considers less than two hours after the initiating event, NUREG/CR-1278, Figure 17-2, page 17-15). The Savannah River State human error data base development for non-reactor nuclear facilities (Benhardt et al. 1994) calculated the failure probability of longer time window tasks. These were called "long-term accident recovery" actions and were defined as "the failure to diagnose a situation and to correctly identify a recovery action when hours to days are available for the recovery". Using THERP fault tree modelling three failure probability values were proposed based on the available time for accident recovery and other conditions such as training, quality of procedures, and stress. As no installation-specific data were available for long time windows tasks, the recommended HEPs are the result of a THERP analysis in which median HEPs are converted into mean HEPs (based on the lognormal distribution for the HEPs) and rounded to 1, 3, or 5 times the appropriate power of ten. The HEPs were thus recommended for the non-reactor facilities (e.g., plutonium storage, waste tanks, solid waste disposal or defence waste processing). These probabilities are presented in Table 3.

Table 3: Recommended human error probabilities for long time windows actions at Savannah River State non-reactor facilities (Benhardt et al. 1994).

Nominal mean value	3.0E-3	EF = 10	Use: 24 to 48 hours for recovery, simple recovery actions
High mean value	1.0E-1	EF = 3	Use: Less than 24 hours for recovery
Low mean value	3.0E-5	EF = 10	Use: Three to seven days for recovery, simple recovery actions

The nominal mean value provided is 3.0E-3. This assumes that (a) recovery actions are to be completed within 24 to 48 hours following the initiating event, (b) stress is moderately high for the operators on shift during the initiating event but decreases to optimal levels for subsequent shifts, (c) there is low dependence on the previous shift, (d) procedures with checklist are

followed, and (e) the second shift personnel might recover any errors made by the previous shift. The high mean value failure probability is $1.0E-1$. It differs by the nominal case by assuming extremely high stress levels due to recovery actions to be completed within a short time frame of approximately 2 to 24 hours and by eliminating the two recoveries modelled in the nominal THERP tree. The low mean value failure probability considers an extended time window of three to seven days and thus optimal stress levels and recovery possibility, and is estimated at $3.0E-5$.

Prolonged available time issue is also related to level 2 PSA since HRA needs to include a more comprehensive and realistic assessment of influences of long-term post-core damage events (ASAMPSA_E, 2015). Long-term post-core damage sequences, with time windows for severe accident management guideline actions spanning from several hours up to 72 hours, invoke new issues regarding the timing of operator actions. For example, in the Fukushima Dai-ichi NPP accident, the opening of containment vent valves was unexpectedly delayed by several hours by: 1) waiting for a nearby town to be evacuated, 2) hardware failures, and 3) harsh environment conditions that developed during the waiting time. For these prolonged scenarios, potential time delays need to be accounted for in a realistic manner. The lack of contingency procedures and pre-staged equipment impacted operator actions, so that operators had to operate outside the procedural space or formal training. Relevant PSFs, such as fatigue (e.g., operators in the Fukushima Dai-ichi NPP event had long shifts with minimal food and rest) and “stress” in a very real sense.

Another potentially important aspect of long-term scenarios is the impact of shift changeover on the reliability of measure. Shift changeovers may lead to a loss of information or situational awareness, thus inducing additional sources of human error. In a longer time scenario, the plant crisis organization would be in place. The potential impacts of multiple decision makers on the performance should be considered realistically.

HRA in a longer time window might be related to knowledge-based decisions and actions for mitigating an accident. Therefore, it should be considered how to systematically analyse knowledge-based decisions and actions in a longer time window. This is considered as one of the needs in level 2 HRA for those post-core damage HFEs.

When there are longer available times, the potential new human actions should also be considered, e.g. recovery and repair actions. The credit and considerations of recovery and repair actions are discussed in section 2.4.

It is noted that ASME PRA standard requires to account for any dependency between the HFE for operator recovery and any other HFEs in the sequence, scenario, or cut set to which the recovery is applied (ASME/ANS RA-Sa-2009). NPSAG HRA dependencies project reports provide good summaries on how to assess the dependency level and how to consider use of minimum values for joint HEPs (He et al. 2016 & 2017).

2.6 Risk and reliability analysis methods

In this section, mathematical methods and models applicable to risk and reliability analysis for accident scenarios with long mission times are considered. In practice, they are methods that enable crediting repairs and recoveries, and also facilitate modelling situations where the order of events can vary and the order matters. Dynamic PSA methods fit these requirements.

Static fault tree and minimal cut set based techniques have significant limitations in modelling time related aspects. In level 1 PSA, the static and simplified approach has mostly been considered sufficient, but when modelling longer time windows, the limitations of the approach become more evident. In level 2 PSA, there has been more variety in the use of methods because of the dynamic behaviour of severe reactor accidents. Some level 2 PSAs rely on static event trees and fault trees, whereas some other level 2 PSAs use more advanced event tree techniques (ASAMPSA2 2011, Tyräinen et al. 2016, Guigueno et al. 2016).

In principle, PSAs could be made more realistic by using dynamic methods (Aldemir 2013), e.g. dynamic and simulation-based event trees (Metzroth 2011, Karanki et al. 2015, Queral et al. 2018, Tyrväinen et al. 2016, Tyrväinen & Karanta 2019). On the other hand, the static approach has significant benefits, such as minimal cut sets, reasonable computation times, transparency of the model and easiness of the modelling. In addition, change of the method would be laborious. In the short run, it could be more realistic to consider incorporation of dynamic analyses to the static models, e.g. by more accurate computation of minimal cut set frequencies by dynamic methods (Bäckström et al. 2018), use of time-dependent basic events (USNRC 2017) or crediting convolution (USNRC 2017, Smith 2016). Convolution could be used e.g. in the combined analysis of emergency diesel generator failure times and offsite power recovery time (USNRC 2017). Complementary dynamic analyses could also be used to improve PSA models in some specific scenarios (Mandelli et al. 2019).

Markov models are a dynamic method to model state transitions of systems and components (Bucci et al. 2008). Markov models are particularly useful in modelling repairs and recovery actions. Markov models are likely not practical for plant-wide modelling, but can be effective and accurate in the analysis of individual systems. Hassija et al. (2014) present a good example on the application of Markov models to a long time window scenario with time-dependent success criterion.

Initiators and All Barriers (I&AB) is a dynamic methodology developed by EDF (Industrial Risks Management Department, France) and which is implemented in RiskSpectrum® PSA. It enables taking repair into account in a practical way in a full scope PSA application at the same time as you can actually define sequence specific time intervals referring to the available time to repair failed components until the undesirable end state occurs. Implementation of I&AB in RiskSpectrum® PSA is further described in (Bäckström et al. 2018). The PSA model is solved in the same way as for a static PSA, resulting in a minimal cut sets list to be quantified. These cut sets are then quantified using the I&AB method. This method is an analytic conservative approximation of the continuous time Markov chains for the cut set. It captures the most important dynamic behaviour of a failure mode (that is, the first-order dependence between failures of barrier components), while offering an approximate analytical method.

2.7 Reliability data

Basic events in PSA are normally divided into unavailability (because the equipment is undergoing testing or maintenance), failure to start or change state, and failure to run (after successfully starting) or maintain state to the end of the required mission time (NUREG-6823, 2002).

The basic event representing fail to run (FTR) is typically modelled with the reliability model 'mission time' which calculates the failure probability based on the failure rate and the mission time.

$$Q(t) = q + (1 - q)(1 - e^{-\lambda T_m}) = 1 - (1 - q)e^{-\lambda T_m}$$

where $Q(t)$ is the failure probability of the component; q is mission time independent failure probability for the component; λ is failure rate; T_m is the mission time.

This reliability model is used for most components, which have a mission time. Failures are assumed Poisson distributed which implies that the failure rate λ does not change during the mission time. The model also assumes that the component cannot be repaired within the mission time period (non-repairable).

In reality, failure rates of some components are not constant. The assumption of constant failure rate might particularly be unrealistic in long mission time scenarios.

For emergency diesel generators (EDGs), the available data are in general applicable only for short mission times since the operating experience is mainly based on the performed periodical tests, when the diesels functioning duration is generally short.

Grant et al. (1999) used reported EDG failures from tests performed at plants that reported under RG-1.108 requirements during the study period (1987-1993). These tests required the EDGs to run for 24 hours. There were 27 FTR events observed in the cyclic surveillance test data. The duration of the EDG run times prior to the failure of the EDG were reported in 19 of the licensee event reports. Based on analysis of these data the study concluded that three distinct failure rates existed. The failure rate during the first half an hour was $2.5\text{E-}2$ per hour. The failure rate decreased significantly to $1.8\text{E-}3$ per hour for the period between 0.5 hours and 14 hours. For periods greater than 14 hours, the failure rate again decreased to $2.5\text{E-}4$ per hour. Figure 3 illustrates the estimation of the three different failure rates.

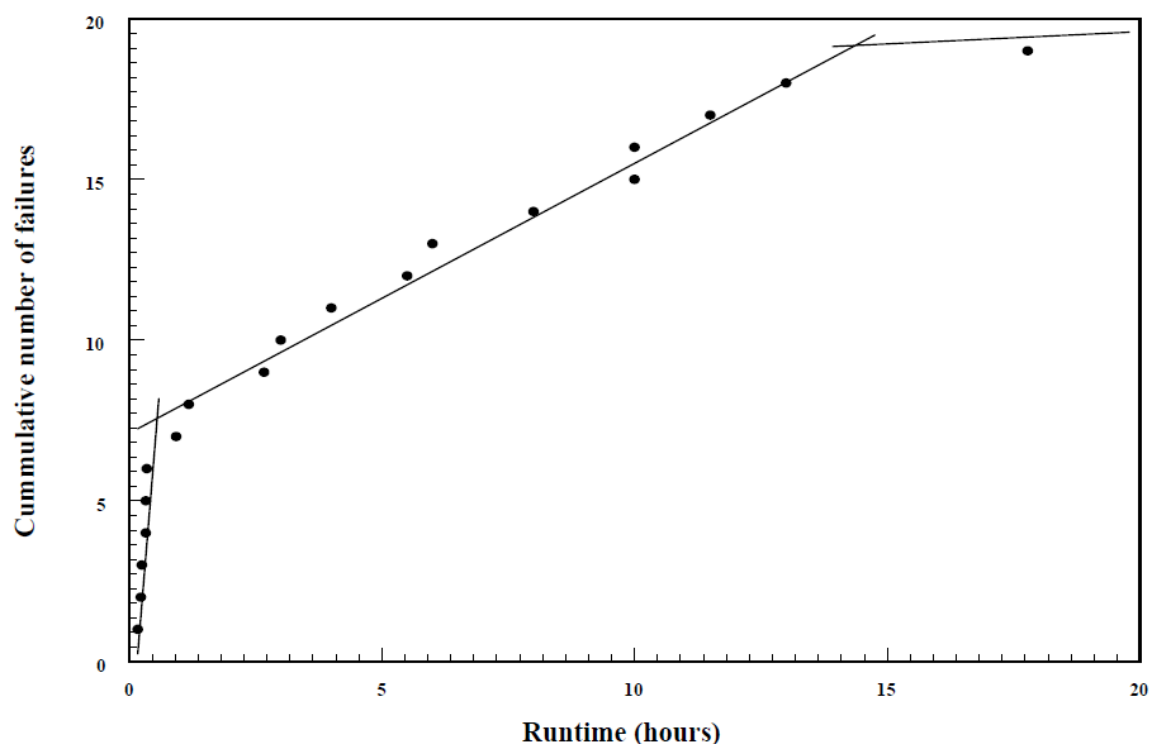


Figure 3: Cumulative number of EDG FTR events observed during the cyclic surveillance tests as a function of the time of the failure (Grant et al. 1999).

They commented that the early, middle, and late failures seem to correspond in part to different failure mechanisms. The change in the failure rate per hour was linked to a change in the mechanism of the EDG train failures. That is, the cooling subsystem dominated the early failures, accounting for about one-third of all the failures that occurred during the first half an hour; the electrical and fuel subsystems combined account for half of the failures in the period between 0.5 hours and 14 hours; and beyond 14 hours the only failure observed occurred in the electrical subsystem.

In comparison to the EDG failure data applied in US PSA or individual plant examination (IPE) study, approximately 80% of the PSA/IPEs reviewed by Grant used a single hourly failure rate for the entire mission time. The average failure rate for these PSA/IPEs is $5.9\text{E-}3$ per hour. The remaining PSA/IPEs differentiated between less than one hour and greater than one hour failure rates. The average failure rate based on the less than an hour PSA/IPE data is $1.1\text{E-}2$ per hour. The greater-than-one-hour average failure rate based on the PSA/IPE data is $2.3\text{E-}3$ per hour.

The plant-specific estimates of failure to run probability were calculated for the respective mission times postulated in the PSA/IPE. The mission times postulated in PSA/IPE accidents were 6, 8, and 24 hours. Susquehanna assumed a 72-hour mission time, but details on how this was factored into the EDG failure probability estimate are not available. The RG-1.108 values for Susquehanna are calculated for a 24 hour mission time. Even though the IPE stated a 72-hour mission time, RG-1.108 data is restricted to less than a 24-hour run time. Extrapolating the FTR probability to 72 hours was not done since the failure data was based solely on the cyclic surveillance tests of 24-hour endurance run. The Palo Verde IPE utilized a 7-hour mission time as their success criteria. The RG-1.108 values for Palo Verde are based on an 8-hour mission time.

In T-book for Nordic countries, one mean failure rate is provided for the diesel generator spurious stop. The critical failures included in the spurious stop have been the following: leakage in various forms, spurious trip for long start-up time or high voltage due to erroneous or incorrectly adjusted relays. The mean failure rate is around $1\text{E-}3/\text{h}$ level for Nordic plants. If this failure rate was used for scenarios of a longer mission time, the EDG failure probability would be quite high.

It is necessary to look at the whole EDG train boundaries for the prolonged mission time, as the root causes must be addressed as a part of the analysis. The boundary of the EDG train includes

- the diesel engine,
- electrical generator,
- generator exciter,
- output breaker,
- load shedding and sequencing controls,
- EDG room heating/ventilating subsystems,
- the exhaust path,
- lubricating oil,
- fuel oil subsystem (including all storage tanks permanently connected to the engine supply),
- the starting compressed air subsystem.

The fuel capacity of the day fuel tank and the large external storage tank need to be considered. The large external storage tanks have a capacity for several days of system operation. The day tank typically has capacity to operate the engine for 4 to 6 hours (Grant et al. 1999).

A more recent study is INL/EXT-14-31133 where a performance evaluation of EDGs using Equipment Performance and Information Exchange data from 1998 through 2012 and maintenance unavailability performance data using Mitigating Systems Performance Index Basis Document data from 2002 through 2012. The failure types studied are failure to start, failure to load and run and failure to run >1 hour. The results indicate that the failure rate during the first hour is more than three times greater than the failure rate after the first hour.

2.8 Epistemic uncertainty

Uncertainties are generally divided into two types: aleatory and epistemic. For the PROSAFE project mainly the epistemic uncertainty is of interest, since the aleatory uncertainty (stochastic uncertainty) describes the randomness that is the basis of events and phenomena.

Epistemic uncertainty refers to uncertainties related to a lack of knowledge, information or methods, also called "State-of-knowledge uncertainty" (NUREG-1855). This type of uncertainty can be identified, valued and reduced and is therefore relevant for all areas of the PROSAFE literature study. Three different definitions of epistemic uncertainty are presented in Table 4.

Epistemic uncertainty is normally divided into three groups:

- Parametric uncertainty
- Model uncertainty
- Completeness uncertainty

For the areas of the literature study, parametric uncertainty mainly relates to uncertainties in reliability data, parameter values in thermo-hydraulic success criteria calculations and human reliability calculations. Model and completeness uncertainties exist more or less in all tasks, though with emphasis on model uncertainty.

The need to address model and/or completeness uncertainties concerning e.g. stable end state, success criteria and mission time was identified in (ASAMPSA_E 2015) but also recognised to be significantly harder to quantify than parametric uncertainty. Although it was stated to require alternative logic models, it was found necessary to include in the PSA.

Related to the areas of the PROSAFE literature study, the following high level or supporting requirements can be found in the ASME/ANS RA-S-2008:

- HLR-SC-B: The thermal/hydraulic, structural, and other supporting engineering bases shall be capable of providing success criteria and event timing sufficient for quantification of [core damage frequency] CDF and [large early release frequency] LERF, determination of the relative impact of success criteria on SSC and human actions, and the impact of uncertainty on this determination.
- HR-D6: PROVIDE an assessment of the uncertainty in the HEPs in a manner consistent with the quantification approach. USE mean values when providing point estimates of HEPs.
- HR-G8: Characterize the uncertainty in the estimates of the HEPs in a manner consistent with the quantification approach, and PROVIDE mean values for use in the quantification of the PRA results.
- HLR-QU-E: Uncertainties in the PRA results shall be characterized. Sources of model uncertainty and related assumptions shall be identified, and their potential impact on the results understood.
- HLR-LE-F: The quantification results shall be reviewed, and significant contributors to LERF, such as plant damage states, containment challenges, and failure modes, shall be identified. Sources of model uncertainty and related assumptions shall be identified, and their potential impact on the results understood.

NUREG-1855 gives guidance on how to address the different epistemic uncertainties in PSA applications, it does however not give guidance on how to treat uncertainties within specific areas, e.g. safe and stable end state or acceptance criteria. Though the presented methodology should in large be applicable also for plant PSA.

A possible approach for evaluating uncertainties in assumptions related to the success criteria definition is described in NUREG/CR-7177, where the effect of variations in MELCOR modelling assumptions on figures-of-merit for level 1 PSA is investigated and also the choice of core damage surrogates. It was found that some particular modelling assumptions can have significant impact, e.g. break size and location, number of ruptured steam generator tubes, reactor power level at the time of trip, timing of early operator actions, time of battery depletion, behaviour of turbine-driven systems after battery depletion; and stochastic failure in the open or partially open position of relief valves.

NUREG/CR-7177 also presents a MELCOR uncertainty analysis for a loss of feedwater scenario and compare the results with a corresponding uncertainty analysis performed with MAAP code, without finding any significant differences in terms of the fraction of accident simulations predicted to result in core damage.

Table 4: Definitions for epistemic uncertainty.

Source	Definition
ASME/ANS RA-S-2008	<p><i>“the uncertainty attributable to incomplete knowledge about a phenomenon that affects our ability to model it. Epistemic uncertainty is reflected in ranges of values for parameters, a range of viable models, the level of model detail, multiple expert interpretations, and statistical confidence. In principle, epistemic uncertainty can be reduced by the accumulation of additional information. (Epistemic uncertainty is sometimes also called ‘modeling uncertainty.’)”</i></p> <p>Source of model uncertainty: “a source that is related to an issue in which there is no consensus approach or model and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, introduction of a new initiating event).”</p>
NUREG-1855	<p><i>“Model uncertainty is related to an issue for which no consensus approach or model exists and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, and introduction of a new initiating event). A model uncertainty results from a lack of knowledge of how structures, systems and components (SSCs) behave under the conditions arising during the development of an accident.”</i></p>
NUREG-2122	<p><i>“Variability in an estimate because of the randomness of the data or the lack of knowledge.”</i></p> <p><i>“Parameter uncertainty is the uncertainty in the values of the parameters of a model represented by a probabilistic distribution. Examples of parameters that could be uncertain include initiating event frequencies, component failure rates and probabilities, and human error probabilities that are used in the quantification of the accident sequence frequencies.”</i></p> <p><i>“Completeness uncertainty is caused by the limitations in the scope of the model, such as whether all applicable physical phenomena have been adequately represented, and all accident scenarios that could significantly affect the determination of risk have been identified.”</i></p>

3. Questionnaire

A questionnaire was prepared for the stakeholders of the project. It covers the same areas as the literature survey in the previous section. The questions are presented in Appendix. Five nuclear power plant companies, two nuclear safety regulators, and one nuclear fuel and waste management company answered to the questionnaire. This section presents a summary of questionnaire results. The section is divided into subsections according to the areas of the questionnaire.

3.1 Safe, stable state

The respondents provide different definitions of safe and stable end state (SSES) with variations regarding content, areas of applicability (e.g. PSA, deterministic safety analysis) and level of detail. Two organizations have no definition that is applied in PSA.

SSES for PSA level 1. Most definitions of SSES for PSA level 1 agree on requiring successful reactor shutdown and secured decay heat removal. Many also require reactor subcriticality and water supply for 24 hours, which is the time window mentioned when explicitly included in the definitions (i.e., in 50% of the responses).¹ One organization also includes in the definition of safe state the requirement of a non-pressurized reactor and of a leak-tight containment in LOCA scenarios. When SSES definitions for spent fuel are provided they refer to sufficient cooling to maintain stable temperature (and subcriticality). Three organizations also mention a general definition that “safe state is an operating state that minimizes the risk of a radiological accident.” One of the organizations mentions it only in relation to deterministic safety analyses.

Some organizations specifically define the concepts “controlled”, “safe” and “final safe state”, but also here differently. A controlled state requires reactor shutdown (and subcriticality for one organization) and decay heat removal. Safe state is achieved when the reactor is also depressurized and can be kept in controlled state as long as the safety demands of the event remain. From a safe state it is possible to return to normal operation or proceed to the final safe state. Final safe state is when the subcritical reactor’s residual heat is removed with a good margin and the safety demand caused by the event no longer exists. The reactor can be depressurized and the core removed. One organization applies the definition of controlled state to the successful end states in PSA instead of the definition of safe state.

One organization specifies a definition for spent fuel so that “safe state means that operations with handling of the fuel are able to end such that the spent fuel is in fuel pools or in another position where it can be stored safely with respect to cooling and criticality.”

SSES for PSA level 2. In broad terms PSA level 2 definitions assume a SSES when a major release to the atmosphere has ceased within 24 hours from the event start. The reactor is in “controlled state”, which implies core/debris decay heat removal secured, core/debris temperatures stable or decreasing, no risk of re-criticality, and no significant volumes of fission products being released, and, in addition, any remaining release is minor (the pressure inside the containment is low enough if the containment is not leak-tight). Two organizations specify the parameters for the size of a small release (e.g., less than 0.1% of volatile / non-volatile fission products of the hearth inventory of a 1800 MW type reactor; reactor subcritical with reactor pressure vessel (RPV) temperature under 100 °C). Some organizations do not necessarily consider the successful end states in PSA level 2 as stable and safe states, but as controlled states.

¹ One organization used to distinguish between safe states (“ok” end states in the PSA event tree) recognizing that although a core is kept stable and cooled within the time frame, discharge of primary coolant to the atmosphere may still occur and/or core damage might occur later, if additional recovery actions to establish long-term cooling are not performed. This distinction is no longer applied.

SSES in deterministic analysis. In deterministic analysis the definitions of “stable state” refer to an operating mode where the radiological consequences of an accident are under allowed values. The situation is under control when the transient is over. More specifically, the definitions refer to the following set of physical conditions/parameters:

- reactor shut down and non-pressurised
- fuel covered with water
- no boiling
- decay heat removal secured (e.g., RPV temperature below 100 °C)
- reactivity control established (e.g., effective multiplication factor of less than 0.995)
- manual cool down
- shutdown margin < 5% (safe state)

For events that include severe core damage additional criteria of the SSES are:

- water-covered core/debris
- residual heat removal / long term cooling for the core/debris,
- debris temperatures stable or decreasing
- no risk of re-criticality
- no significant volumes of fission products being released.

The successful transition from a controlled state to a safe state is usually grounded on a qualitative analysis, and specific “stable states” are defined for each analysis.

Half of the organizations did not see needs for improvement concerning the definition of safe, stable state. One organization stated that more exact definition would increase realism, but it is a matter prioritization. For regulators, it would be easier to interpret results if all utilities used the same definitions. One organization stated that “there is some ambiguity how the definitions for safe state versus controlled state are used. It is also somewhat unclear how the definitions should be applied for other operational states than at-power and for non-reactor nuclear facilities.”

3.2 Success criteria

All organizations stated that a more realistic consideration and modelling of time related dependencies of success criteria could in general be beneficial for the PSA, especially for long time windows but also within the normal 24 hours mission time, and it could improve the use of PSA applications and decision making based on PSA input.

Success criteria is in general developed based on a conservative approach, though several organizations stated that they aim for a best estimate approach. The main concern with regard to long time windows was how to take into account that success criteria may change over time.

The deterministic acceptance criteria used in developing success criteria for the different safety functions are very similar among the different organizations (e.g. maximum fuel cladding temperature < 1204 °C), except for one organization that applies a criteria of max 1000 °C for 10 min in a core node during the time course studied. Concerning spent fuel pool some

organizations only applied fuel covered in water as acceptance criteria, while others also considered avoidance of boiling.

Failures of system functions are either assumed to occur immediately after initiating event or divided into a few steps related to battery capacity times (mainly considered for electrical SSCs). This is either way conservative, and with increased mission times the conservatism will also increase (relatively). Change of success criteria over time was only considered by two different organisations for one case each.

The computer codes used for calculating success criteria were considered realistic for long time windows by two organisations, though the codes had not been verified for long time windows.

Most organizations analysed other end states than core damage, mainly boiling of spent fuel pool or condensation pool, but partial core damage was only analysed by one organization and in that case for level 2 (limited core melt).

3.3 Mission times

Most organizations use mission time of 24 hours in level 1 PSA. One organization uses 20 hours. In level 2 PSA, the used mission times vary from 24 hours to 48 hours (including also some mission times between those values). One organization performs level 2 analysis 24 hours from the onset of the release, which varies. Longer mission times are considered for shutdown states and spent fuel pool analyses. Some organizations use shorter mission times in loss of offsite power scenarios and for batteries. One organization models some actions outside the defined time windows. A special case is an interim storage facility for spent fuel, for which mission time of 720 hours is used.

If safe, stable state is not reached at an analysis end point, some organizations extend the mission time and some do not.

Some organizations identified some possibilities to change mission times. Longer mission times could be used for seismic events. Shorter mission times could be used for diesel generators, because loss of offsite power can be shorter than 24 hours, and for some supporting systems, such as ventilation systems.

Challenges related to mission times include:

- Estimation of failure probabilities in long time window scenarios (see Sections 3.4, 3.5 and 3.7)
- Changing success criteria
- Modelling different mission times increases the model complexity and the number of basic events
- Some components, such as motor operated valves, need to be actuated several times during the mission time
- Possible measures that can be taken after a long time period may not be possible to analyse with credibility
- How to deal with extremely long mission times

3.4 Recoveries and repairs

Most organizations model some recovery actions. The recoveries that are modelled are typically selected based on their importance for the results and available time. Most organizations did not specify which recoveries are modelled. Recoveries of core cooling and pressure relief in level 2 PSA are examples that were mentioned.

Repairs are modelled typically only in long mission time scenarios, such as level 2 PSA and spent fuel pool analyses.

Recoveries and repairs are modelled in PSA either as separate basic events or they are included in the probabilities of basic events representing execution errors. One organization specifies that they have a fault tree dedicated for repair events, which appears as an event tree layer.

Dependencies between recovery and repair actions and other human actions are generally not taken into account. One organization assumes that recovery/repair is either completely dependent of the related human action or independent. However, if a recovery failure is included in an execution failure, the available time after the execution failure is analysed.

Errors of commission are not considered in any of the modelled recovery actions.

To estimate recovery and repair probabilities, HRA methods, plant data and expert judgements are used. HRA methods that are used include Enhanced Bayesian THERP (Holmberg 2019) and modified accident sequence evaluation program (ASEP) HRA procedure (NUREG/CR-4772).

Estimation of recovery and repair probabilities is considered a challenge in long time window scenarios. Their modelling also increases model complexity. Modelling of dependencies between recoveries and repairs and other human actions could make the analysis more realistic. Examples of actions that could be modelled in the future include repair of diesel generators, and events related to residual heat removal, water supply and power supply.

3.5 HRA methods

The HRA methods used are SPAR-H (NUREG/CR-6883), THERP (NUREG/CR-1278), Enhanced Bayesian THERP (Holmberg 2019) and ASEP-HRA (NUREG/CR-4772). Some organizations use a combination of two or more of these methods and some organizations use a modified version of the method.

Some organizations only consider the diagnosis part for most actions inside the main control room. One organization states that the reason for this is that the failure of execution is considered to be negligible compared to the diagnosis part. One organization assumes that simple and short executions (regardless of location) can be included in the diagnosis part. Sometimes the diagnosis and execution parts are modelled as one common basic event, and sometimes it is split up into two separate basic events. Practices of taking recovery into account vary: some organizations take it into account in both diagnosis and execution parts, some do not at all.

In general, no specific modelling is used for human actions with long time windows, but the available time is taken into account as one of the PSFs in most HRA methods. Also, in some organizations expert judgements and modified or extrapolated values from the ASEP-method are used. One organization noted that they do not think that enough credit is given for very long time windows with the method that they are using (SPAR-H). Another organization comments that they see the need for guidance on how to estimate the effect of the available time on the human error probability.

Some organizations do not use a lower limit for the failure probability and one of them also notes that this assumption is motivated by their PSA study. Other organizations use 1E-4 as a lower limit and one organization sets the limit to 1E-6.

Most organizations do take concurrent and competing activities into consideration when the HEP is calculated, but some do not.

All organizations that responded to the question “Are any human actions with long time window modelled” do include such human actions in their PSA. Examples of such actions are actions that are required late in level 1 PSA, actions in PSA level 2 or actions/repairs related to spent fuel pools. For fuel pools the available time for some of the modelled actions are in the scale of several days or weeks.

Most organizations intend to consider different crews and shift changes. Sometimes this is included when evaluating the PSFs and sometimes a qualitative assessment is made based upon expert judgements.

The main area for development that is identified is how to credit the long available time for manual actions and what other factors to take into account. Some organizations indicate that the used methods do not completely cover these manual actions with long available time in a satisfactory manner.

3.6 Methods to model time-dependencies

Different time windows for the return of offsite power are modelled in several PSAs. One organization models different diesel generator failure times with separate basic events. One organization considers the order of cable failures in fire PSA, because the impact depends on the order, but implements different scenarios simply with individual basic events in the PSA model.

Current PSA methods are generally considered sufficient to produce the required results. Some organizations however do not consider current methods sufficient to model various time-dependencies. One organization mentioned that challenging time-dependent scenarios do not play an important role in overall results.

Dynamic methods have not been used in PSA analyses. Reasons include lack of tool support and amount of effort needed.

Needs to model of time-dependencies include

- Modelling of dynamic success criteria
- Modelling of failure times in common cause failures (it is conservative to assume that all occur at the same time)
- Passing timing information from level 1 to level 2
- Modelling of core reflooding in critical time window for hydrogen production
- Modelling of fast and slow impacts of fires (some safety features may be available early in the scenario, but fail later due to fire)

3.7 Reliability data

Most organizations have not considered increasing or decreasing failure rates during an accident. Some organizations have modelled different failure rates for diesel generators depending on the mission time. Diesel generators have in those cases been modelled with a higher failure rate for short mission times, i.e. the failure rate for diesel generators decreases for longer time windows. In the study presented in INL/EXT-14-31133, it is shown that the failure rate for diesel generators decrease with operating time.

One organization notes that modelling long mission times is a challenge since it makes failures almost inevitable, even if this is not the experience of the operator. There is a perceived discrepancy between reality and PSA in this issue.

Some organizations comment that there is a need to identify component groups and failure modes for which non-constant failure rates should be used. One suggestion is that it should be evaluated if such data could be presented in the T-book.

3.8 Epistemic uncertainty

There were rather few answers to the questions covering uncertainty even though it is a recognised area of concern.

A few organizations stated that uncertainties concerning definition of safe and stable end state, success criteria, mission time and reliability data were small within 24h, but also that a conservative approach had been used. One organization stated that mission times much longer than 24h used in their analyses are used due to requirements and not related to realistic time to reach a safe and stable end state, and hence not an epistemic uncertainty.

Large uncertainties were said to be found mainly concerning scope of HRA for long term scenarios with associated failure probabilities, and reliability data for active equipment with mission times longer than 24 hours. Also, the choice of recovery actions to include, and hence also the number of recovery actions, in the analyses was identified to increase uncertainty.

3.9 Analysis cases to study within the project

Spent fuel pool accident scenarios were proposed by several organizations. Two organizations stated that HRA should play an important role in the analysis. Long term loss of offsite power and external hazard impacting sea water intake were also mentioned. One organization proposed that a normal accident scenario (e.g. loss of coolant accident or transient) with mission time of 24 hours would be modelled more realistically taking into account dynamic success criteria and repairs. The same organization also proposed analysis of a scenario with extended mission time considering reaching the safe, stable state.

4. Conclusions

This report presents the results of a state of the art review on long time windows in PSA and important related topics. The review consists of a literature survey and a questionnaire for the stakeholders of the PROSAFE project. The topics covered in this report are: safe, stable state; success criteria; mission times; recoveries and repairs; HRA methods; risk and reliability analysis methods; reliability data; and epistemic uncertainty. The literature related to long time windows appears to be very limited, because PSA is typically limited to the mission time of 24

hours. Scenarios with long mission times are generally recognised as a challenging topic that should be studied more.

Ideally, successful PSA sequences should lead to a safe, stable end state. Therefore, the definition of the safe, stable state can affect success criteria and mission times. However, in practise, that does not seem to be usually the case. Success criteria analyses focus typically on avoiding core damage within fixed time window rather than reaching safe, stable state. Different safe (stable) state definitions found from the literature and specified by the stakeholders of the PROSAFE project vary significantly, and there does not seem to be common way to define successful PSA end states. Some also apply the concept of a controlled state in PSA instead of safe state.

Success criteria are in general calculated, and applied, in the PSAs with a conservative approach, i.e. by using conservative acceptance criteria while not addressing partial core damage, and assuming time independent success criteria during the accident sequence. This agrees with state-of-practice in the international PSA community, though several literature sources identify the need for consideration of time dependencies, both within 24 hours mission time and beyond. The collected opinion from the questionnaire is that the PSA will benefit from an advance in methodologies in order to reach a more realistic consideration and modelling of time related dependencies of success criteria.

In level 1 PSA, mission time of 24 hours is usually applied for most safety functions and components. In level 2 PSA, the mission time is typically 24 hours or 48 hours, but in some cases, even 72 hours has been applied. In spent fuel pool analyses, longer mission times may also be used, e.g. 72 hours. It is usually not accurately analysed how long it takes to bring the plant to a safe, stable state. Extending the mission time is however generally recommended if plant conditions are not stable at the end of normal mission time. Modelling of different mission times is considered challenging because it increases the model complexity and the number of basic events.

Some recovery actions are usually modelled in PSA, e.g. for offsite power, emergency diesel generators and emergency core cooling. Repairs are usually not modelled in PSA, except when long mission times are modelled. Probabilities of recoveries and repairs are estimated based on HRA methods, plant data or expert judgements depending on the case. Dependencies between recoveries, repairs and other human actions are usually not taken into account. Modelling of recoveries and repairs is considered a challenge because it significantly increases the model complexity.

Category C HFEs with long time window usually exist in PSA. Examples are human actions that are required late in level 1 PSA, actions in PSA level 2 or actions/repairs related to spent fuel pools. Their available time windows are different, with a range from a few hours to a few days (or even a few weeks for spent fuel pool). TRC from THERP/ASEP (or a modified curve, or combined with a low cut off value) is still commonly used to derive the diagnosis HEPs of these HFEs. SPAR-H uses the PSF available time as one of the eight PSFs and the maximum multiplier for available time PSF is 0.01. In general when the available time is long, the HEPs will reach the applicable boundary of the HRA methods and there is no further guidance available to consider the effects of the extra time and the related issues e.g. shift change, fatigue, coordination and communication, etc. Thus there is a clear need of better guidance on how to estimate the effect of the long available times on the HEPs.

A large number of references on dynamic PSA methods can be found from the literature. Such methods could potentially make PSA more realistic. However, according to the questionnaire answers, current PSA methods, event trees and fault trees, are considered sufficient to produce the required results. Some time-dependencies, like dynamic success criteria, have however been considered challenging to analyse using the current methods, and there is need to study suitable approaches for modelling such time-dependencies.

It has been shown in a few different studies that failure rates of some components are not constant over time. Time-dependencies in reliability data are often not considered in PSA. It is a challenge especially when long mission times are modelled as the probability of failure is perceived as being much too conservative if these kinds of dependencies are not considered.

Epistemic uncertainty is by the Nordic PSA community in general considered to be an important area of improvement within the PSA, which concur with the result of the literature survey. The answers to the epistemic uncertainty area of the questionnaire was however few, which may be an indication that the area is pre-maturely addressed and that the other areas addressed by PROSAFE, and which the uncertainty area concern, must first be further elaborated. The literature study also shows that there are rather few references available on the subject and that it is recognized as a difficult area to address.

The objective of the questionnaire was to map current practice and difficulties within the areas of the literature survey and to identify the stakeholders view on the prioritized areas for research and development. Based on the results of the questionnaire the following contents for the continuation of the PROSAFE 2019 are proposed:

- **Work package 2, Safe and Stable State.**

The answers of the questionnaire show that the stakeholders do not see this as a prioritized area, see section 3.1. However, the project can see some challenges in performing the activities of work package 3 without addressing the definition of safe and stable state, especially for e.g. analysis of spent fuel pool. Based on the above, we propose that no new activities in this area are included in the 2019 activities, but that a definition of Safe and Stable State is developed within work package 3 in order to support the work there, and the area will then be further considered when planning the 2020 activities of PROSAFE.

- **Work package 3, Methodologies**

The activity is proposed to cover the following areas:

- Modelling of sequences with long time windows. This will mainly address events for the spent fuel pool but also core related events requiring mission times longer than 24 hours.
- HRA methodology for actions with long grace times.
- Consideration of repair of failed equipment.
- Time window modelling with respect to credit of repairs, dynamic success criteria and failure data.
- Failure data. The area will be shortly addressed by identification of needed development, e.g. prioritized component types.

- **Work package 4, Pilot Studies**

The purpose of the pilot studies is to evaluate the feasibility of the proposed methods in WP3. Real case studies can point out significant issues for the method development work of WP3. For this purpose the generic model from the DIGREL project (Authen et al. 2015) will be used, and complemented with a model for the spent fuel pool. Apart from this, the Ringhals 3/4 model of the spent fuel pool may also be used. The Pilot studies are carried out in close cooperation with the utilities which are the owners of NPP PSAs.

References

Aldemir, T. (2013). A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants. *Annals of Nuclear Energy*, 52, 113-124.

American Nuclear Society (2009), ASME/ANS RA-S-2009 Standard for level 1/large early release frequency probabilistic risk assessment for nuclear power plant applications. New York.

American Nuclear Society (2009), ANS/ASME-58.22-2014 Requirements for Low Power and Shutdown Probabilistic Risk Assessment. New York.

ASAMPSA2 (2011). Best-practices guidelines for L2PSA development and applications, Volume 1 - General. Euratom.

ASAMPSA2 (2013). Best-practices guidelines for level 2 PSA development and applications, Volume 2 - Best practices for the Gen II PWR, Gen II BWR L2PSAs. Extension to Gen III reactors. Euratom.

ASAMPSA_E (2015). Lessons of the Fukushima Dai-ichi accident for PSA. Euratom.

Authén, S., Holmberg, J.-E., Tyrväinen, T., Zamani, L. (2015). Guidelines for reliability analysis of digital systems in PSA context – Final Report. NKS-330, Nordic nuclear safety research (NKS), Roskilde.

Ayyub, B. (2001). Elicitation of expert opinions for uncertainty and risks. CRC Press.

Benhardt, H.C., Held, J.E., Olsen, L.M., Vail, R.E., Eide, S.A. (1994). Savannah River Site human error data base development for nonreactor nuclear facilities. WSRC-TR-93-581, Savannah River Technology Center, Aiken, SC.

Bucci, P., Kirschenbaum, J., Mangan, L.A., Aldemir, T., Smith, C., Wood, T. (2008). Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliability Engineering and System Safety*, 93 (11), 1616-1627.

Burgazzi, L., Davidovich, N., Meloni, P., Lo Frano, R. (2014). Risk analysis of nuclear power plants against external events. Italian National Agency for New Technologies (ENEA), Report RdS/PAR2013/089, Rome.

Bury, K. (1999). Statistical distributions in engineering. Cambridge University Press.

Butler, J.S., Kapitza, D., Martin, R.P., Seifae, F., Sundaram, R.K. (2010). Analysis and justification of MAAP4.0.7 for PRA level 1 mission success criteria. *Nuclear Technology*, 170, 244-260.

Bäckström, O., Bouissou, M., Gamble, R., Krcal, P., Sörman, J., Wang, W. (2018). Introduction and Demonstration of the I&AB Quantification Method as Implemented in RiskSpectrum PSA. 14th International conference on probabilistic safety assessment and management (PSAM14), Los Angeles, CA, 16-21 September, 2018. Paper #203.

Cooke, R. (1991). Experts in uncertainty - opinion and subjective probability in science. Oxford University Press.

Guigueno, Y., Raimond, E., Duflo, N., Tanchoux, V., Rahni, N., Laurent, B., Kioseyan, G. (2016). Severe accident risk assessment for NPPs: Software tools and methodologies for

level 2 PSA development available at IRSN. 13th International conference on probabilistic safety assessment and management (PSAM13), Seoul, Korea, 2-7 October, 2016.

Grant, G.M., Poloski, J.P., Luptak, A.J., Gentillon, C.D., Galyean, W.J. (1999). Reliability Study: Emergency Diesel Generator Power System 1987-1993, NUREG/CR-5500, Vol. 5, INEL-95/0035, Idaho National Engineering and Environmental Laboratory, Idaho Falls, ID.

Hassija, V., Senthil Kumar, C., Velusamy, K. (2014). Markov analysis for time dependent success criteria of passive decay heat removal system. *Annals of Nuclear Energy*, 72, 298-310.

He, X. (2016). Dependencies in HRA. NPSAG REPORT 41-001:01.

He, X. (2017). Dependencies in HRA, Phase II. LRC Report 212171_R001.

Holmberg, J.-E. (2019). HRA methodology for Forsmark NPP and Ringhals NPP. NPSAG report 53-002, The Nordic PSA Group.

Idaho National Laboratory (2014). Enhanced Component Performance Study: Emergency Diesel Generators 1998-2012. INL/EXT-14-31133

International Atomic Energy Agency (1996). Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants: A Safety Practice. Safety Series No. 50-P-10.

International Atomic Energy Agency (2006). Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1511, Vienna.

International Atomic Energy Agency (2016). Attributes of full scope level 1 probabilistic safety assessment (PSA) for applications in nuclear power plants. IAEA-TECDOC-1804, Vienna.

International Atomic Energy Agency (2016). Safety of nuclear power plants: Design, Specific safety requirements No. SSR-2/1 (Rev. 1). IAEA-SSR-2/1, Vienna.

International Atomic Energy Agency (2019). Deterministic safety analysis for nuclear power plants, Specific safety guide No. SSG-2 (Rev. 1). IAEA-SSG-2, Vienna.

Jacquemain, D. et al. (2018). Status report on long term management and actions for a severe accident in a nuclear power plant. NEA/CSNI/R(2018)13, Nuclear Energy Agency. Draft. Limited availability.

Jung, W., Park, J. (2019). Time-reliability correlation for the human reliability analysis of a digitalized main control room. International conference on applied human factors and ergonomics (AHFE 2019), Washington DC, July 24-28, 2019. pp. 88-94.

Karanki, D.R., Kim, T.-W., Dang, V.N. (2015). A dynamic event tree informed approach to probabilistic accident sequence modeling: Dynamics and variabilities in medium LOCA. *Reliability Engineering and System Safety*, 142, 78-91.

Kichline, M. (2018). Human reliability analysis for using portable equipment [presentation]. United States Nuclear Regulatory Commission, EPRI HRA for FLEX workshop, February 28 - March 1, 2018.

Mandelli, D., Wang, C., Alfonsi, A., Smith, C., Youngblood, R., Aldemir, T. (2019). Mutual integration of classical and dynamic PRA. International topical meeting on probabilistic safety assessment and analysis (PSA 2019), Charleston, SC, April 28 – May 3, 2019.

Ma, Z., Buell, R. (2016). Safe and stable state in SPAR model event trees. Idaho National Laboratory, INL/LTD-16-38575, Idaho Falls.

Metzroth, K.G. (2011). A comparison of dynamic and classical event tree analysis for nuclear power plant probabilistic safety/risk assessment [dissertation]. The Ohio State University, Ohio, USA.

Meyer, M., Booker, J. (2001). Eliciting and analysing expert judgment - a practical guide. Society for Industrial and Applied Mathematics.

Munier, N. (2014). Risk management for engineering projects – procedures, methods and tools. Springer International Publishing Switzerland.

Norman, E., Brotherton, S., Fried, R. (2008). Work breakdown structures – the foundation for project management excellence. John Wiley & Sons.

O'Connor, P., Kleyner, A. (2012). Practical reliability engineering, 5th edition. John Wiley & Sons.

O'Hagan, A., Buck, C., Daneshkhah, A., Eiser, R., Garthwaite, P., Jenkinson, D., Oakley, J., Rakow, T. (2006). Uncertain judgments - eliciting experts' probabilities. John Wiley & Sons.

Ortiz, N. R., Wheeler, T. A., Breeding, R. J., Hora, S., Meyer, M. A., Keeney, R. L. (1991). Use of expert judgment in NUREG-1150. Nuclear Engineering and Design, 126, 313-331.

Queral, C., Gomez-Magan, J., Paris, C., Rivas-Lewicky, J., Sanchez-Perea, M., Gil, J., Mula, J., Melendez, E., Hortal, J., Izquierdo, J.M., Fernandez, I. (2018). Dynamic event trees without success criteria for full spectrum LOCA sequences applying the integrated safety assessment (ISA) methodology. Reliability Engineering and System Safety, 171, 152-168.

Parry, G., et al. (1992). An Approach to the Analysis of Operator Actions in PRA. EPRI TR-100259, Electric Power Research Institute, Palo Alto, CA.

Radiation and Nuclear Safety Authority (STUK) (2018). Radiation and nuclear safety authority regulation on the safety of a nuclear power plant. Regulation STUK Y/1/2018, Helsinki.

Smith, C.L., Wood, T., Knudsen, J., Ma, Z. (2016). Overview of the SAPHIRE probabilistic risk analysis software. 13th International conference on probabilistic safety assessment and management (PSAM13), Seoul, Korea, 2-7 October, 2016.

Swain, A.D. (1987). Accident sequence evaluation program human reliability analysis procedure. NUREG/CR-4772, United States Nuclear Regulatory Commission, Washington DC.

Tyrväinen, T., Karanta, I. (2019). Dynamic containment event tree modelling techniques and uncertainty analysis. VTT Technical Research Centre of Finland Ltd, VTT-R-06892-18, Espoo.

Tyrväinen, T., Silvonen, T., Mätäsniemi, T. (2016). Computing source terms with dynamic containment event trees. 13th International conference on probabilistic safety assessment and management (PSAM13), Seoul, Korea, 2-7 October, 2016.

United States Nuclear Regulatory Commission (1977). Periodic testing of diesel generator units used as onsite electric power systems at nuclear power plants, Revision 1. Regulatory guide 1.108, Washington DC.

United States Nuclear Regulatory Commission (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. NUREG/CR-1278, Washington DC.

United States Nuclear Regulatory Commission (2003). Handbook of parameter estimation for probabilistic risk assessment. NUREG/CR-6823, Washington DC.

United States Nuclear Regulatory Commission (2005). Good Practices for Implementing Human Reliability Analysis (HRA). NUREG-1792, Washington DC.

United States Nuclear Regulatory Commission (2005). The SPAR-H Human Reliability Analysis Method. NUREG/CR-6883, Washington DC.

United States Nuclear Regulatory Commission (2006). Evaluation of human reliability analysis methods against good practices. NUREG-1842, Washington DC.

United States Nuclear Regulatory Commission (2010). Confirmatory thermal-hydraulic analysis to support specific success criteria standardized plant analysis – Surry and Peach Bottom. NUREG-1953, Washington DC.

United States Nuclear Regulatory Commission (2012). EPRI/NRC-RES Fire Human Reliability Analysis Guidelines. NUREG-1921, Washington DC.

United States Nuclear Regulatory Commission (2013). Glossary of risk-related terms in support of risk-informed decision making. NUREG-2122, Washington DC.

United States Nuclear Regulatory Commission (2014). Compendium of analyses to investigate select level 1 probabilistic risk assessment end-state definition and success criteria modeling issues. NUREG/CR-7177, Washington DC.

United States Nuclear Regulatory Commission (2017a). Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making. NUREG-1855, Washington DC.

United States Nuclear Regulatory Commission (2017b). Risk assessment of operational events, Handbook, Volume 1 - Internal events, Revision 2.02. Washington DC.

Williams, T. (2002). Modelling complex projects. John Wiley & Sons.

Working group on risk assessment, WGRISK (2017). Probabilistic safety assessment insights relating to the loss of electrical sources. Nuclear Energy Agency, Organisation for Economic Co-operation and Development, NEA/CSNI/R(2017)5.

Appendix: Questionnaire

The list of questions included in the questionnaire is presented below.

Part 1: Safe, stable state

- 1.1 How is safe, stable end state defined in your organization in
 - a. level 1 PSA (full-power, low power and shutdown)?
 - b. level 2 PSA?
 - c. deterministic safety analyses?
 - d. If safe, stable end state has not been defined for some of the above analyses, can you present some ideas on how the safe, stable state could be defined for those?
 - e. What is the reasoning behind the safe, stable end state definition? Why such plant state is considered safe?
- 1.2 Do you have deterministic acceptance criteria on some physical parameters for defining the safe, stable state?
 - a. If yes, specify the criteria. How were the criteria decided? Are different criteria used for different scenarios?
 - b. If not, which parameters should/could be considered when developing such criteria? If you have suitable limit values (even roughly) in mind, e.g. based on your thermo-hydraulic analyses used to determine success criteria for safety functions, please specify. Should the criteria depend on the scenario that is analysed or not?
- 1.3 Can you provide examples on how the safe, stable state definition is applied in practice, e.g. in specific accident scenarios?
- 1.4 Do you identify any problems in the current definitions of safe, stable states, or needs for improvement?

Part 2: Success criteria

- 2.1 Defining success criteria:
 - a. What are your main principles for defining success criteria?
 - b. Are your success criteria conservative or based on best estimates?
 - c. What are your main concerns regarding (long) time windows?
- 2.2 What deterministic acceptance criteria / limit values are used in developing success criteria for each key safety function of core and containment at:
 - a. Power operation?
 - b. Low power and shutdown?
 - c. Spent fuel pool?
- 2.3 Describe if and how you consider time dependencies (mission time) when addressing success criteria for system functions in your PSA, e.g.:

- a. What kind of assumptions are made about failure times of other systems failing in the same scenario? Do you e.g. assume failures at the earliest possible time, when failures could occur at any time point during e.g. 24 hours?
- b. Are there cases where initial success criterion could change during the accident, e.g. from 2-out-of-4 to 1-out-of-4, to account for increased margins to acceptance criteria later in the sequence? Have such cases been modeled or could there be need to model such scenarios?

2.4 Are success criteria for support systems

- a. calculated using supporting computer codes? If not, what are they based on?
- b. coherent with time dependencies considered for success criteria of the supported front line systems, or conservatively assigned based on “worst-case”?

2.5 Concerning the computer codes you use for calculating success criteria:

- a. Have they been qualified/verified for long time windows?
- b. Do you think that the results for long time windows are (or would be) realistic?

2.6 Are partial core damage, damaged/uncovered fuel in spent fuel pool (criticality) or other end states than core damage analyzed?

- a. If yes, explain when and how success criteria are developed.
- b. If no, explain why.

2.7 Do you think a more realistic consideration/modelling of time dependencies of success criteria would be beneficial for the PSA?

- a. If no, please state why.
- b. If yes, please state in which areas.

Part 3: Mission times

3.1 Defining mission times:

- a. What are your main principles for defining mission times?
- b. Do you extend the mission time when/if a safe and stable end state is not reached within the pre-defined mission time?

3.2 Do you apply other mission times than 24 hours?

- a. In which scenarios?
- b. In which scenarios could it be necessary to consider longer or shorter mission times?
- c. Have you modelled different mission times for the same safety function/system/component in different accident scenarios? If yes, how?

3.3 Challenges related to mission times:

- a. What kind of challenges do you experience related to determination of the mission times?

- b. What kind of practical challenges do you experience related to modelling of different mission times, e.g. related to PSA software or model complexity?

Part 4: Recoveries and repairs

- 4.1 Are there any recovery/repair actions modelled in the plant HRA and PSA? If yes, please explain:
 - a. How the recovery/repair actions are identified? What criteria need to be fulfilled in order to consider recovery/repair actions and under which circumstances?
 - b. How the actions are quantified, including the method, the considered factors, etc.?
 - c. How the dependencies are considered between the recovery/repair action and the related human actions in the PSA?
 - d. Are errors of commission considered in recovery/repair actions?
 - e. How are the recoveries/repairs and their effects modelled in PSA models?
- 4.2 Are there any challenges that have prevented you from crediting some recovery or repair actions?
- 4.3 Which recovery and repair actions could be credited in your PSA model, particularly if longer mission times would be used?

Part 5: HRA methods

- 5.1 In general terms describe the Type C (post-initiator) HRA methodology in your plant PSA (level 1 & 2, internal and external event), including:
 - a. Which HRA method(s) is used? Have you modified the method(s) for your purposes?
 - b. Are "Diagnosis" and "Execution (post-diagnosis)" always addressed separately in the quantification? If no, please explain why. If yes, is recovery in general considered for both "Diagnosis" and "Execution (post-diagnosis)"?
 - c. If applicable, also describe briefly how the time effects are considered in HRA.
- 5.2 Please provide information on how the human actions with expansive available time (available time is much longer than the nominal time required) are currently quantified, e.g.:
 - a. How the expansive time is considered in the diagnosis and execution?
 - b. If limiting human error probability value is defined and applied?
 - c. If the impact of concurrent and competing activities is considered?
 - d. The impact of other performance shaping factors on the time available.
 - e. If staff (MCR, TSC, ERO) operates differently as opposed to short available time scenarios?
- 5.3 Are any human actions with long time window modelled, especially in the plant level 2 PSA?

- a. If yes, please provide some example human actions and explain how this has been considered in the quantification.
- b. If no, please explain why there are no such human actions.

5.4 Are there any scenarios in the PSA model (level 1 and level 2) where different crews are considered in connection with a long time window? If yes, can you describe:

- a. e.g. personnel outside main control room, technical support organization, crisis management organization, firefighters, etc.
- b. How this is quantified/taken into account?
- c. Have you considered changes of shifts (one shift replacing another)? If yes, how have you taken these into account in the model?

Part 6: Methods to model time-dependencies

6.1 Modelling timings:

- a. Have different possible timings of any events, e.g. failure times, been modelled in level 1 or in level 2? If yes, provide examples and information on how the modelling has been done.
- b. Could there be need to model timings, e.g. failure times, more in level 1 or in level 2? If yes, please provide examples.
- c. Do you consider current methods sufficient for modelling timings? If there are problems, what are the main problems?

6.2 Dynamic methods:

- a. Have you used any dynamic methods in your analyses concerning e.g. recoveries, repairs, failure times or long time windows?
- b. If you have used dynamic methods, which ones have you used and what is your experience about those (benefits, downsides, etc.)?
- c. If you have not used dynamic methods, why not (no regulatory requirement, no important scenarios where they would be needed, difficult to understand, tedious to model, lack of tool support)?
- d. Do you have suggestions on what methods should be studied to model time aspects better in PSA?

Part 7: Reliability data

7.1 In reality, failure rates of components may increase or decrease during an accident.

- a. Have you identified such cases? Do you have evidence for that in operational experience?
- b. What failure data have you used in this context?
- c. Do you consider time-dependent failure rates in PSA? How?
- d. Do you consider time-dependent failure rates an important issue in long mission time scenarios?

- e. Do you know failure data references for long mission time scenarios?

Part 8: Epistemic uncertainty

8.1 How do you consider completeness and model uncertainty with regard to:

- a. Definition of safe, stable end state?
- b. Developed success criteria?
- c. Assumed mission times?
- d. HRA methods and probabilities?
- e. Recoveries?
- f. Reliability data?
- g. Quantification methods?

8.2 What is your area of biggest concern regarding epistemic uncertainty?

Part 9: Analysis cases

9.1 Can you specify example scenarios that you think should be analysed in the PROSAFE project?